Restoring a Blue Prism Environment

To restore a Blue Prism environment, users must have generated backups. This guide provides information on how to back up and subsequently restore a Blue Prism environment using backed up content. It covers the following scenarios:

- Backing up and restoring process automations and associated information. Learn more...
- Performing a full system backup and restore into either an existing Blue Prism environment or a new Blue Prism environment. Learn more...
- Information is also included about detecting encryption schemes and locating certificates. Learn more...

Back up and restore process automations

Process automations developed in Blue Prism comprise any number of processes, business objects, and embedded application models. They can be backed up and restored separately from other areas of the system.

For backing up full systems, see Back up and restore the full system.

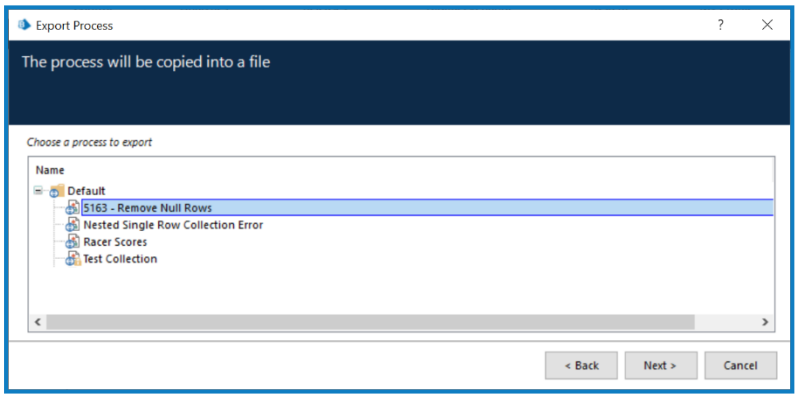
Backup

Objects and processes can be exported individually or as part of a release package for multiple objects/processes with additional components.

For more information about the automate.exe commands in the following sections, see the Blue Prism online help.

1. **Individual items – File > Export**

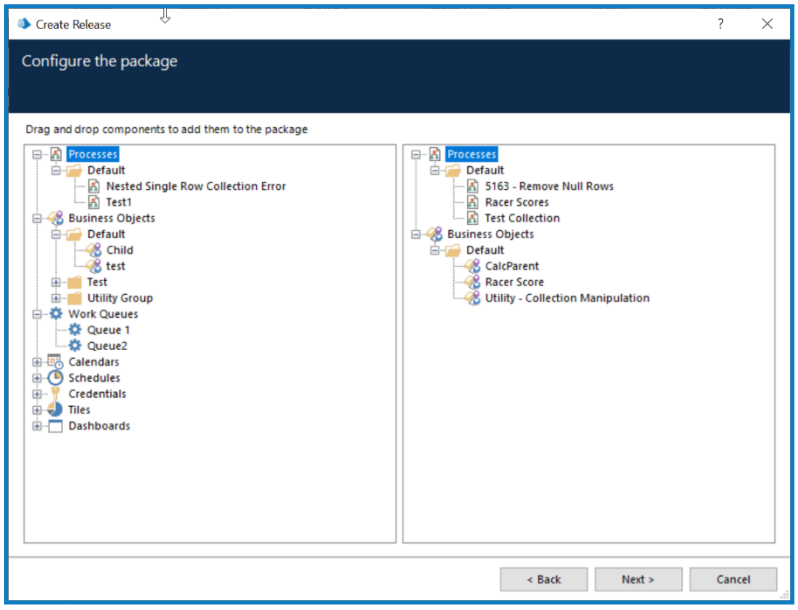
   In Studio, select **File** > **Export** > **Process/Object**, select all the objects or processes to be exported and the file destination.
   This can also be achieved programmatically by using `automatec.exe /export`.



2. **Multiple items – Release package**

   Release packages are configured in Blue Prism and contain any mixture of objects and processes, and related file types.
   Once a package has been defined it is ready for export. The package will automatically be updated to include the latest version of each item as it is exported.
   The export can be done manually or programmatically by using `automatec.exe /exportpackage`.

   Use the **Find References** feature, accessed by right-clicking a process or object in the navigation tree, to add a selection of all related records to the release package.



Related file types that can also be exported within a release package include:

- **Calendars** – calendars configured for use by schedules set on holidays, working, and non-working days.
- **Dashboards** – the layout and presentation settings of each tile on the dashboard. The data source settings must be explicitly exported if required. No reporting data is exported.
- **Credentials** – credential records and their settings, but excluding sensitive information such as passwords and secrets.
- **Schedules** – schedule information such as which process automations should be triggered at a given time. No schedule log history is exported.
- **Tiles** – data sources settings, and query-information used by dashboards. No reporting data is exported.
- **Work queues** – work queue records and their settings. No work queue items are exported.

> The export does not typically represent a full backup of these items, but only their configuration settings.

Restore

Use **File > Import** to import or restore objects, processes, or release packages into an existing Blue Prism environment.

If any conflicts are detected during the import, e.g. if an item with the same name already exists, there are options to overwrite, create a duplicate, or ignore the item.

This can also be achieved programmatically:

- When importing objects or processes use: `automatec.exe /import`.Use `/overwrite` to force objects or processes to overwrite any of the same names already in the store.
- When importing release packages use: `automatec.exe /importpackage`.

The default behavior when conflicts are detected as part of a package import process is described below:

Conflict	Outcome
An item in the release package has the same name/ID as an item of the same type that already exists in the store.	The item in the store will be overwritten.
An object or process will be overwritten but the item in the release package is marked as published, and the item in the store is not marked as published.	The item in the store will be marked as published.
An object or process will be overwritten but the item in the store is marked as retired.	The item in the store will stay retired.
The release package includes a tile, but the user does not have permission to import tiles.	The entire package will fail to import.
The release package includes a credential record, but the Blue Prism environment is not correctly set up to store credentials (i.e. no default encryption scheme is configured).	The entire package will fail to import.
An object in the release package matches the name or ID of a process in the store.	The entire package will fail to import.
A process in the release package matches the name or ID of an object in the store.	The entire package will fail to import.

Restrictions

There are several restrictions or considerations when importing objects, processes or release packages into an existing Blue Prism environment:

- The target version of Blue Prism must be the same or newer than the source version.
- Object, process and release package files only contain the information as outlined – typically they do not contain data such as credential secrets, or work queue items.

Back up and restore the full system

It is possible to do a backup and restore of the full system either to achieve a rollback to a previous state; OR to create a new Blue Prism environment using pre-existing configuration and data.

All file paths assume a default installation of Blue Prism. Paths must be adjusted accordingly for custom installations.

Backup

For each component there are several items that can be backed up: some of them are essential to ensure that a full system restore can take place, whereas others are optional and will simply reduce the effort in achieving a restore.

- Interactive clients – items requiring mandatory backup.
- Runtime resources – No items requiring mandatory backup.
- Application servers – Mandatory backup required to prevent data loss.
- Database – Mandatory backup required to prevent data loss.

Interactive clients

Interactive clients do not contain any Blue Prism information that must be backed up in order to be re-built or re-configured.

	Detail	Instructions
Mandatory	None	N/A
Optional	**Connection configuration information** Contains the connection string information for each Blue Prism environment.	Take a copy of **Automate.config** located here: C:\ProgramData\Blue Prism Limited\Automate V3 **Frequency:** Following a configuration change. **Secure backup location required?** Only if the runtime resource connects to the Blue Prism environment using Blue Prism native authentication.

Runtime resources

Runtime resources do not contain any Blue Prism information that must be backed up in order to be re-built or re-configured.

A runtime resource will typically be configured with an operating system, configuration, required software, and have connectivity to the network and line of business applications. It is essential that the backup and recovery plans include the ability to recreate these devices with this same base configuration.

	Detail	Instructions
Mandatory	None	N/A
Optional	**Connection configuration information** Contains the connection string information for each Blue Prism environment.	Take a copy of **Automate.config** located here: C:\ProgramData\Blue Prism Limited\Automate V3 **Frequency:** Following a configuration change. **Secure backup location required?** Only if the runtime resource connects to the Blue Prism environment using Blue Prism native authentication.
	Windows Service login accounts The accounts used by Blue Prism services such as Login Agent services.	Take a screenshot or make a note of the login accounts used by the relevant services within the Services console on the relevant devices.
	Login Agent configuration information Contains the connection and authentication information that ensures a Blue Prism runtime resource is available to orchestrate a login when the device is in a logged-out or locked state.	Take a copy of **LoginAgentService.config** located here: C:\ProgramData\Blue Prism Limited\Automate V3 Only valid if Login Agent is used as part of the deployment. **Frequency:** Following a configuration change. **Secure backup location required?** Only if the Login Agent runtime resource connects to the Blue Prism environment using Blue Prism native authentication.
	Start-up procedure The automated steps that contain the connection and authentication information which ensures a Blue Prism runtime resource is started and available to work when the device is logged in.	Depends on the start-up procedure. Commonly requires the Group Policy Management settings to be backed up; otherwise it may be a backup of the device's scheduled task settings. **Frequency:** Following a configuration change. **Secure backup location required?** No

Application server

Application servers contain information that are required in order to be re-built. If this data is lost, it will not be possible to recover some of the data within the database – although it will not cause damage to the system.

	Detail	Instructions
Mandatory	**Encryption scheme information** (if stored on the application server) Contains critical information about the encryption schemes used to protect data at rest.	Only required if one or more encryption schemes are configured to store the key on the application server.* If Store Keys separately in individual files = yes* • Take a copy of the folder structure and *.bpk files in the configured location. If no • Take a copy of automate.config located here C:\ProgramData\Blue Prism Limited\Automate V3 *See the Additional information on page 13 section for further guidance. **Frequency:** Following a configuration change. **Secure backup location required?** Yes
	Configuration file certificate (with private key) (if used – v6.7+ only) Provides the information needed to decrypt the config files that contains the encryption scheme information.	Only required if the Blue Prism server is configured to protect the configuration files with a certificate, AND if the back up of encryption scheme information occurred after the certificate has been applied.* Use Certificate Manager on each application server to export the certificate, along with its private key, whose thumbprint matches the one configured in the BPServer.exe. *See the Additional information on page 13 section for further guidance. **Frequency:** When the certificate changes. **Secure backup location required?** Yes
Optional	**Connection configuration information** Contains the connection string information for each Blue Prism environment.	Take a copy of **Automate.config** located at C:\ProgramData\Blue Prism Limited\Automate V3 **Secure backup location required?** Yes
	Windows Service login accounts The accounts used by Blue Prism services such as Blue Prism server services.	Take a screenshot or make a note of the login accounts used by the relevant services within the Services console on the relevant devices. **Secure backup location required?** No

Database

The Blue Prism database contains information that must be backed up in order to be able to restore a Blue Prism environment.

If backing up the database to create a new copy of the Blue Prism environment where it is likely that the linked runtime resources will no longer be valid, it is strongly recommended that the runtime resources connected to the environment are safely shut down before taking the database backup.

If the database is used to create a new Blue Prism environment and the previously connected runtime resources will still be used with the old environment, or if they cannot be accessed from the new environment, it may be necessary to contact Blue Prism Support for assistance following the database restore if the runtime resources have not been safely shut down prior to taking the backup.

	Detail	Instructions
Mandatory	**Blue Prism database** Contains all settings and data used by the Blue Prism platform including, but not limited to: objects; processes; credentials, and their secrets; work queues; work queue items; user and access information; historical processing; and audit information.	Blue Prism supports both Simple and Full SQL recovery modes and it is recommended that the benefits of each is reviewed to ensure the method chosen is appropriate to the criticality of the solution. If the database has been set to use a Full recovery model, it is important that regular transaction log backups take place. **Backup Frequency:** Regularly – to suit the criticality of the environment. **Secure backup location required?** Yes
Optional	None	

Additional considerations

While not required, consider setting up a central repository to store all the installer executables that you use as part of setting up Blue Prism. This will likely include Blue Prism, Login Agent, as well as components such as MAPIEx and JAB. It may also include items such as SQL Server, SQL Management Studio, mainframe emulators, remote access agents, and other end user applications.

Restore

A full system restore can be achieved using the backed up mandatory items listed above. The guide describes two restore scenarios:

- Restoring an environment to use a database backup
- Recreating a new environment from backups

Restoring an environment to use a database backup

To revert a Blue Prism environment to use a previously backed up database, follow the steps below:

1. Stop or disconnect all Blue Prism devices that connect indirectly to the database – this includes any device that connects via a Blue Prism application server such as runtime resources and interactive clients.
2. Stop or disconnect all Blue Prism devices that connect directly to the database. Commonly this will just require the Blue Prism application server service to be stopped on each application server. These will also need to be stopped where runtime resources or interactive clients establish a direct connection to the database.
3. Use SQL Server tools to:
    a. Stop all connections to the database.
    b. Back up the current database to a safe place. See Additional information on page 13 for further guidance.
    c. Restore the previously backed up database. See Additional information on page 13 for further guidance.
4. If the restored database was created when using an earlier version of Blue Prism, reconfigure each Blue Prism component with the version that aligns to this database.
5. The database version can be found within the BPADBVersion table, and can be matched to the correct Blue Prism version within the release notes.
6. Restart and reconnect the devices that connect directly to the database.
7. Restart and reconnect the devices that connect indirectly to the database.

Creating a new environment from backups

To create a new environment using backups follow the steps below:

Restore the database

1. Use SQL Server tools to create a new database from the backup.
2. If the database is being used to create a new environment where the runtime resources that were previously connected are no longer valid, the runtime resources will need to be retired.

> If any invalid runtime resources were connected to the environment when the database backup was taken, you may need contact Blue Prism Support to validate that all runtime resources are in an appropriate offline state.

Create the first application server (with Scheduler disabled)

1. Follow the instructions in the installation guide to install a Blue Prism application server.
2. Configure a connection to the restored database:

Using a backup of the Automate.config file from the server	1. Place the file into the default or custom location dependent on your configuration. The default location for the Automate.config file is: C:\ProgramData\Blue Prism Limited\Automate V3 2. If the configuration file was protected using a certificate, import the certificate, with private key, into the local store on the computer. 3. Edit the profile using BPServer.exe and update the database connection settings to direct to the newly restored database.
Without a backup of the Automate.config file from the server	Follow the instructions in the installation guide to create a new profile and configure it to connect to the newly restored database.

3. If the encryption scheme information is held in separate files, place these into a selected location that is accessible to the application server and use BPServer.exe to edit the profile and update the configured location of the stored keys.
4. Validate that the encryption scheme information is valid.
5. In BPServer.exe validate the settings for the selected connection mode, and disable the Scheduler on this device.
6. Set the Blue Prism server service to operate under the selected user context.
7. Start the Blue Prism server service.

Connect the first interactive client

1. Follow the instructions in the installation guide to install a Blue Prism interactive client.
2. Configure a connection to the application server (or database):

Using a backup of the Automate.config file from an interactive client	1. Place the file into the default or custom location dependent on your configuration. The default location for the Automate.config file is: C:\ProgramData\Blue Prism Limited\Automate V3 2. If the interactive client is configured to connect directly to the database, launch the client and update the settings.
Without a backup of the Automate.config file from an interactive client	1. Follow the instructions in the installation guide to create a new profile and configure it to connect to the application server (or database). 2. Review the per-device settings such as whether a personal runtime resource should be started when the client is launched.

3. Launch the interactive client and validate that it can connect and works as expected.

Create the first runtime resource

1. Follow the instructions in the installation guide to install a Blue Prism interactive client.
2. Configure a connection to the application server (or database):

Using a backup of the Automate.config file from a Runtime Resource	1. Place the file into the default or custom location dependent on your configuration. The default location for the Automate.config file is: C:\ProgramData\Blue Prism Limited\Automate V3 2. If the interactive client is configured to connect directly to the database, launch the client and update the settings.
Without a backup of the Automate.config file from a Runtime Resource	1. Follow the instructions in the installation guide to create a new profile and configure it to connect to the application server (or database).

3. Validate that the automatic start-up procedures for the runtime resource are applied.
4. If used, follow the instructions in the Login Agent user guide to reinstall Login Agent and if available overwrite the newly generated configuration file with the backup.
5. Start the runtime resource.
6. Use the interactive client to start a session on the runtime resource to validate its behavior.

Add additional devices as required

Additional application servers, interactive clients and runtime resources can now be added by repeating the steps above for each component.

Clean up actions

Following a full system restore the following recommendations should be reviewed:

- Validate that Blue Prism license terms are not being breached – as the database contains license information, validate that the same license entitlement is not active elsewhere.
- If the runtime resources in the recreated environment have different device names, the following should be carried out by an administrator within the System tab of an interactive client:
  - Reconfigure schedules to use the new names.
  - Reconfigure resource pools (if used).
  - Retire runtime resources that are no longer valid.
- Ensure that organizational local security policy or group policy settings applied to runtime resources are consistent with those applied to the original devices.
- Re-configure any specific network routing that may be required (i.e. if providing programmatic access to the application server or direct to any runtime resources).
- Re-configure any exposed objects or processes as web services.
- Re-establish backup procedures for the new environment.

If any runtime resources connected to the environment when the database backup was generated are no longer valid, you may need contact Blue Prism Support to validate that all runtime resources are in an appropriate offline state.

Re-enable Scheduler (if required)

If the scheduler is required, it must be enabled on at least one Blue Prism application server.

1. Stop the Blue Prism server service.
2. Use BPServer.exe to enable the scheduler.
3. Start the Blue Prism server service.
4. Restart any devices that were connected to the server.

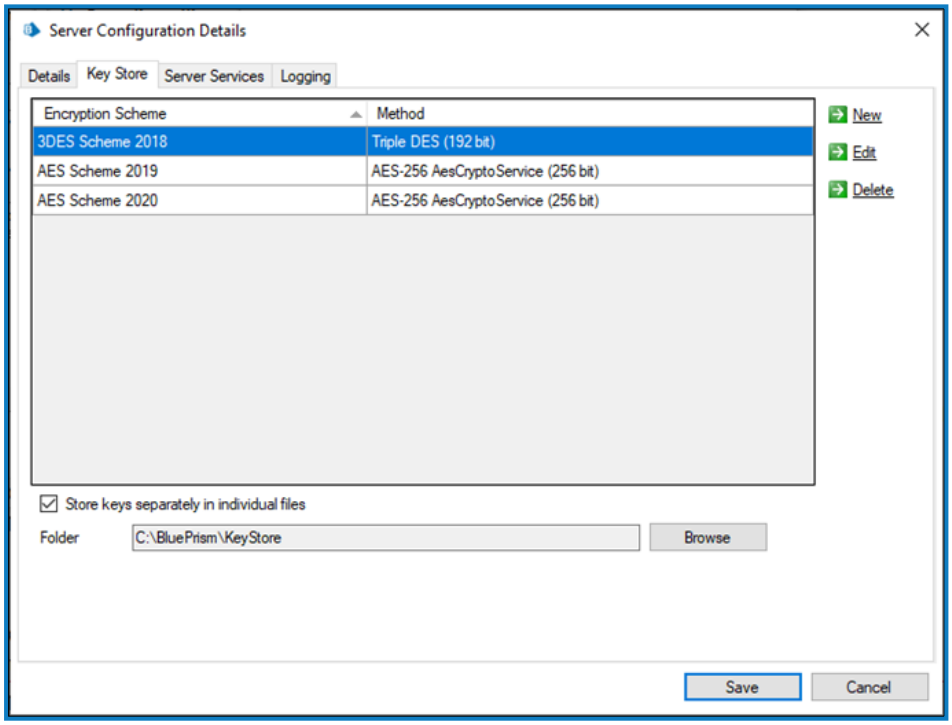
Additional information

Application server

Detecting whether there is encryption scheme information on the application server (and whether they are stored in separate files)

Encryption scheme information can be configured to be stored within the database or the application server (recommended). To see if any encryption scheme information is configured to be stored on the application server:

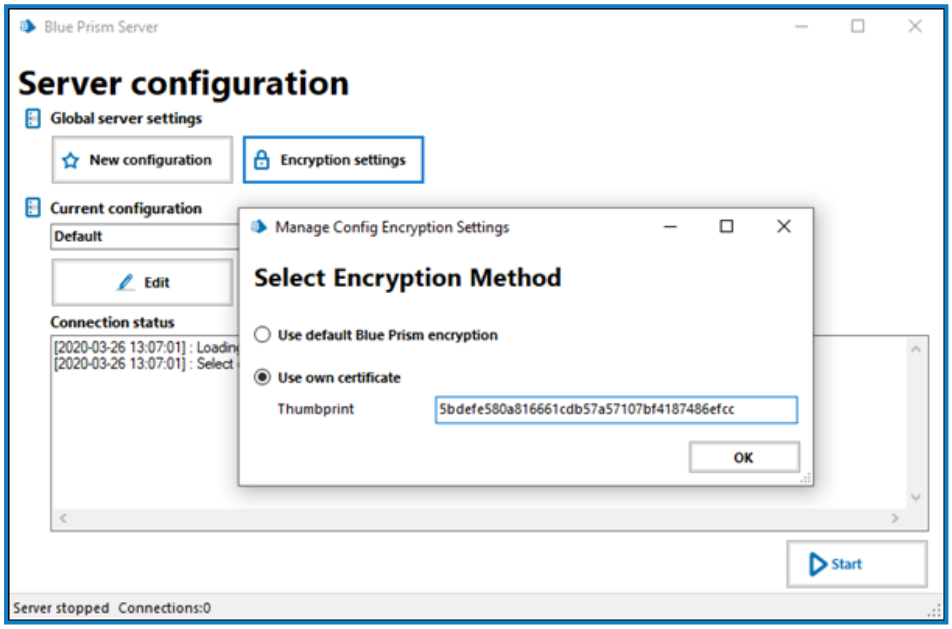
1. Open BPServer.exe and edit the appropriate profile.
2. Click **Key Store**.
3. If there are any entries, then encryption scheme information is stored on the application server.
4. If the option **Store keys separately in individual files** is selected and a folder path displays, then the encryption scheme information will be stored away from the default file in the specified folder path.



Locating the certificate used to protect the application server configuration file

A feature introduced in Blue Prism v6.7 allows users to select to encrypt the Blue Prism application server configuration using a deployed certificate. To detect whether this has been configured:

1. Open BPServer.exe and click **Encryption Settings**.
2. If the option **Use own certificate** is selected, then encryption is applied and the thumbprint will indicate which certificate in the local store is used.
3. Use the thumbprint in the search utility in the device's local certificate store to find the certificate. (Search based on the SHA1 Hash field.)



Database

Backing up a SQL Server Database

To back up a SQL Server database, follow the instructions provided by Microsoft:

https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/create-a-full-database-backup-sql-server?view=sql-server-ver15

Restoring a SQL Server Database

To restore a SQL Server database using SQL Server Management Studio, follow the instructions provided by Microsoft:

https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/restore-a-database-backup-using-ssms?view=sql-server-ver15